



<p>(51) 国際特許分類6 H04L 12/40, 9/00</p>	<p>A1</p>	<p>(11) 国際公開番号 WO98/48543</p> <p>(43) 国際公開日 1998年10月29日 (29.10.98)</p>
<p>(21) 国際出願番号 PCT/JP98/01837</p> <p>(22) 国際出願日 1998年4月22日 (22.04.98)</p> <p>(30) 優先権データ 特願平9/106995 1997年4月24日 (24.04.97) JP</p> <p>(71) 出願人 (米国を除くすべての指定国について) 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP] 〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP)</p> <p>(72) 発明者: および</p> <p>(75) 発明者/出願人 (米国についてのみ) 西村拓也(NISHIMURA, Takuya) [JP/JP] 〒576-0021 大阪府交野市妙見坂6-1-105 Osaka, (JP) 飯塚裕之(IITSUKA, Hiroyuki) [JP/JP] 〒576-0033 大阪府交野市私市6-25-6 Osaka, (JP) 山田正純(YAMADA, Masazumi) [JP/JP] 〒570-0011 大阪府守口市金田町6-24-10 Osaka, (JP)</p> <p>(74) 代理人 弁理士 滝本智之, 外(TAKIMOTO, Tomoyuki et al.) 〒571-8501 大阪府門真市大字門真1006番地 松下電器産業株式会社内 Osaka, (JP)</p>		
<p>(81) 指定国 CN, JP, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p>添付公開書類 国際調査報告書</p>		
<p>(54) Title: DATA TRANSFER METHOD</p> <p>(54) 発明の名称 データ転送方法</p> <div style="text-align: center; margin-top: 20px;"> </div>		
<p>(57) Abstract</p> <p>A data transfer method for preventing the malfunction of the conventional equipment which does not cope with encipherment at the time of transmitting enciphered AV information protected by a copyright through an IEEE 1394 bus. In the method, cipher identification information indicating the state of encipherment of a real data part and the real data part are contained in synchronous data transferred through isochronous communication and encipherment is effected only on the real data part. According to this method, a transmitter transmits cipher identification information indicating the state of encipherment of the real data part contained in the synchronous data together with real data and a receiver which detects the fact that the real data part has been enciphered from the cipher identification information requests the transmitter to send deciphering information and, upon receiving this information from the transmitter in response to the request, decipheres the real data part by using the deciphering information.</p>		

(57)要約

IEEE 1394バスで、著作権により保護されたAV情報を暗号化して送信する際に、暗号化に対応していない従来の機器も誤動作することのないデータ転送方法を提供することを目的とし、アイソクロノス通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行う。

同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データと一緒に送信装置から送信され、実データ部が暗号化されていることをこの暗号識別情報により検出した受信装置が、送信装置に対して復号化情報を要求し、この要求に従って送信装置から送信された復号化情報を受け取った受信装置はこの復号化情報を使用して実データ部の復号化を行うデータ転送方法。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AL	アルバニア	FI	フィンランド	LR	リベリア	SK	スロヴァキア
AM	アルメニア	FR	フランス	LS	レソト	SL	シエラ・レオネ
AT	オーストリア	GA	ガボン	LT	リトアニア	SN	セネガル
AU	オーストラリア	GB	英国	LU	ルクセンブルグ	SZ	スワジランド
AZ	アゼルバイジャン	GD	グレナダ	LV	ラトヴィア	TD	チャード
BA	ボスニア・ヘルツェゴビナ	GE	グルジア	MC	モナコ	TG	トーゴ
BB	バルバドス	GH	ガーナ	MD	モルドヴァ	TJ	タジキスタン
BE	ベルギー	GM	ガンビア	MG	マダガスカル	TM	トルクメニスタン
BG	ブルガリア	GN	ギニア	MK	マケドニア旧ユーゴスラヴィア	TR	トルコ
BF	ブルキナ・ファソ	GW	ギニア・ビサウ		共和国	TT	トリニダード・トバゴ
BJ	ベナン	GR	ギリシャ	ML	マリ	UA	ウクライナ
BR	ブラジル	HR	クロアチア	MN	モンゴル	UG	ウガンダ
BY	ベラルーシ	HU	ハンガリー	MR	モーリタニア	US	米国
CA	カナダ	ID	インドネシア	MW	マラウイ	UZ	ウズベキスタン
CF	中央アフリカ	IE	アイルランド	MX	メキシコ	VN	ヴェトナム
CG	コンゴ	IL	イスラエル	NE	ニジェール	YU	ユーゴスラビア
CH	スイス	IS	アイスランド	NL	オランダ	ZW	ジンバブエ
CI	コートジボワール	IT	イタリア	NO	ノールウェー		
CM	カメルーン	JP	日本	NZ	ニュージーランド		
CN	中国	KE	ケニア	PL	ポーランド		
CU	キューバ	KG	キルギスタン	PT	ポルトガル		
CY	キプロス	KP	北朝鮮	RO	ルーマニア		
CZ	チェコ	KR	韓国	RU	ロシア		
DE	ドイツ	KZ	カザフスタン	SD	スーダン		
DK	デンマーク	LC	セントルシア	SE	スウェーデン		
EE	エストニア	LI	リヒテンシュタイン	SG	シンガポール		
ES	スペイン	LK	スリ・ランカ	SI	スロヴェニア		

420 Rec'd PCT/PTO 25 OCT 1999

明 細 書

データ転送方法

5 技術分野

本発明は、通常のデジタルデータと暗号化されたデジタルデータとが混在するデータを転送するデジタルデータ転送方法に関するものである。

背景技術

- 10 従来のデータ転送方式にはIEEE 1394規格 (IEEE: THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.) を用いたデータ転送方法がある (参考文献: IEEE Std 1394:1995, High Performance Serial Bus)。
- IEEE 1394規格におけるデータ転送には、デジタル映像信号やデジタル音声信号等の同期データの転送に適したアイソクロノス (isochronous) 通信と、制御信号等の非同期データの伝送に適したエイシンクロナス (asynchronous) 通信とがあり、両方の通信はIEEE 1394バス上で使用することが可能である。アイソクロノス通信はいわゆる放送型の通信であり、IEEE 1394バス上の1つの装置が出力するアイソクロノスパケットを、同バス上の全ての装置が受信することができる。これに対してエイシンクロナス通信
- 15 には1対1の通信と1対Nの放送型通信の両方があり、バス上の1つの装置が出力するエイシンクロナスパケットには、そのパケットを受信すべき装置をあらわす識別子が含まれており、その識別子が特定の装置をあらわす時にはその識別子で指定された装置が当該エイシンクロナスパケットを受信し、その識別子がブロードキャストをあらわす時には同バス上の全ての装置が当該エイシンクロナスパ
- 20 ケットを受信する。
- 25

また、IEEE 1394規格に準拠したデータ転送方法を用いて、デジタル音声信号やデジタル映像信号等を転送したり、IEEE 1394バス上に接続された機器間でのデータ伝送を行うための規格として、IEC (IEC: International Electrotechnical Commission 国際電気標準会議) においてIEC 1883規格 (以下、AVプロトコルと称する) が検討されている。AVプロトコルにおいては、映像音声データは図5に示すアイソクロノスパケット内に配置されて転送される。また、アイソクロノスパケットはCIPヘッダ (CIP: Common Isochronous Packet) を含む。CIPヘッダ内には、映像音声データの種別を示す識別情報やアイソクロノスパケットを送信している送信装置の装置番号等の情報が含まれている。

図5はAVプロトコルにて使用されるアイソクロノスパケットのフォーマットをあらわす図である。アイソクロノスパケットは、アイソクロノスパケットヘッダ900、ヘッダCRC901、アイソクロノスペイロード902およびデータCRC903からなる。アイソクロノスパケットヘッダ900にはタグ907が含まれる。タグ907は、その値が1である時には、そのアイソクロノスパケットがAVプロトコルに準拠していることを示す。タグ907の値が1であるとき、すなわちそのアイソクロノスパケットがAVプロトコル準拠のアイソクロノスパケットである時には、アイソクロノスペイロード902の先頭にCIPヘッダ904が含まれる。CIPヘッダ904の中には、当該アイソクロノスパケットを出力している出力装置の識別子であるソースID906が含まれる。また、CIPヘッダ904には、アイソクロノスペイロード902に含まれる実データ905がどのような種類のデータであるかをあらわすFMT908とFDF909が含まれる。映像信号や音声信号のデジタルデータは実データ905に含まれるが、実データ905はアイソクロノスペイロード902にかならず含まれるとは限らず、パケットによっては実データ905を含まずにCIPヘッダ904のみを含

むアイソクロノスペイロード 902 も有り得る。

また、AV プロトコル上で機器制御を行うためのコマンド群として、AV/C コマンドセットがある。(参考文献: 1394 TRADE ASSOCIATION Specification for AV/C Digital Interface Command Set Version 1.0
5 September 13, 1996) これらのコマンドとその応答はエイシンクロナス通信を用いて転送される。

前記従来のデータ転送方法において、著作権保護のためにアイソクロノスペイロード 902 を暗号化したアイソクロノスパケットをアイソクロノス通信で送信しようとする、暗号化されたアイソクロノスペイロード 902 の転送に対応し
10 ていない従来の機器との互換性が保たれなくなる。すなわち、従来の機器は、アイソクロノスペイロード 902 の先頭に CIP ヘッダ 904 が正常に配置されて送信されてくることを前提に作られているので、アイソクロノスペイロード 902 が暗号化されていると、従来の機器では CIP ヘッダ 904 が正常に読み出されず、そのアイソクロノスパケットは AV プロトコルを満たさないものと判断され、そのアイソクロノスパケットを受信した受信装置は正常に動作する
15 ことができなくなる。すなわちその受信装置では実データ 905 に含まれるデータがどのような種類のデータであるかを判別することが不可能であり、当該アイソクロノスパケットを出力している装置を特定することが不可能になるので、かつ当該送信装置に対する各種の問い合わせ等のエイシンクロナス通信を行うこと
20 ができなくなり、受信動作を正常に行うことが不可能になってしまうという課題があった。

また前記従来のデータ転送方法において、送信装置が出力するアイソクロノスパケットを、受信装置が継続して受信している最中にアイソクロノスパケットの暗号化が始まるような場合、従来の機器においては、暗号化が始まった途端に CIP
25 P ヘッダ 904 を正常に読み出すことができなくなり、正常な受信が行えなくな

るという課題があった。

また送信装置が、著作権で保護されている映像音声情報等を暗号化して送信し、正規に認められた受信装置が、その暗号化された映像音声データ等を復号化するためには、送信装置は、正規の受信装置に対して復号のための復号化情報を付与
5 する必要がある。その場合、前記従来のデータ転送方法においては、送信装置が受信装置を特定するには非常に煩雑な手順を実行せねばならない。すなわちアイソクロノスケットには、送信を行っている装置の識別子であるソースID906は含まれるが、どの装置が当該アイソクロノスケットを受信するべきかをあ
らわす情報は含まれておらず、そのため送信装置はどの装置が当該アイソクロノ
10 スケットの受信を行っているかをアイソクロノスケット送信中に調べることはできない。そこで、送信装置が、IEEE1394バス上に接続されている機器のうちのどの機器が受信を行っているかを調べるには、送信装置はバス上の全ての機器に対して受信状態の問い合わせを順次に行わねばならず、復号のための鍵情報を付与する手順が非常に煩雑になるという課題があった。

15 本発明は、前記従来の問題点を解決するもので、暗号化した映像音声情報をアイソクロノス通信で送信する場合にも従来の通信規格を満足し、かつ従来の受信装置が暗号化された映像音声データを含むアイソクロノスケットを受信しても誤動作することのないデータ転送方法を実現することを目的とする。

また本発明は、前記従来の問題点を解決するもので、送信装置が正規の受信装
20 置に復号のための鍵情報を付与する手順を極めて簡素なものにすることが可能なデータ転送方法を実現することを目的とする。

発明の開示

前記従来のデータ転送方法の問題点を解決するために、本発明のデータ転送方
25 法においては、アイソクロノス通信で転送される同期データには実データ部の暗

号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行う。

また前記従来のデータ転送方法の問題点を解決するために、本発明のデータ転送方法においては、同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データと一緒に送信装置から送信され、実データ部が暗号化されていることをこの暗号識別情報により検出した受信装置が、送信装置に対して復号化情報を要求し、この要求に従って送信装置から送信された復号化情報を受け取った受信装置はこの復号化情報を使用して実データ部の復号化を行うことによってデータ転送が行われる。

10 本発明のデータ転送方法においては、同期データを受信した受信装置が、同期データ内に含まれる暗号識別情報を調べ、実データ部が暗号化されていることを検出すると、送信装置に対して実データ部を復号するための復号化情報を要求する。この要求はAV/Cセット中のコマンドによりエイシンクロナス通信を用いて行われ、この要求を受け取った送信装置においては、受け取ったコマンドのパ
15 ケットヘッダを調べることにより、要求を出した機器すなわち受信装置が特定される。ここで特定された受信装置に対して送信装置が復号化情報をエイシンクロナス通信によりコマンドで付与することにより、送信装置が受信装置に復号のための復号化情報を付与する手順が極めて簡素なデータ転送方法を実現できる。

また本発明のデータ転送方法においては、同期データの暗号化は実データ部のみに対して行われ、同期データには実データ部の暗号化状況を示す暗号識別情報が含まれる。これにより、CIPヘッダは暗号化されずにそのまま転送されるので、従来の装置がこれらの暗号化された同期データを受信しても誤動作することはない。すなわち、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が暗号化された同期データを受信しても誤動作する可能性の無いデータ転
25 送方法を実現できる。

また本発明のデータ転送においては、送信装置の送信している同期データを受信装置が継続的に受信している最中に、同期データの暗号化が始まったとしても、C I Pヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できる。

5

図面の簡単な説明

図1は本発明の実施形態におけるC I Pヘッダのフォーマットを表す模式図、

図2は本発明の実施形態における送信装置と受信装置との機能を表すブロック図、

10 図3 Aは本発明の実施形態におけるA K Eステータスコマンドのフォーマットを表す図、

図3 Bは本発明の実施形態におけるA K Eステータスコマンドに対するA K Eレスポンスのフォーマットを表す図

15 図3 Cは本発明の実施形態におけるA K Eコントロールコマンドのフォーマットを表す図

図4は本発明の実施形態における送信装置と受信装置との間で伝送されるエイシンクロナスパケットの伝送手順を表す模式図、

図5は従来のデータ転送方法におけるアイソクロノスパケットのフォーマットを表す図。

20

発明を実施するための最良の形態

以下、本発明の第一の実施形態について、図面を参照しながら説明する。

図1は本発明の実施形態において転送されるアイソクロノスパケットのペイロード部の形式を表した図である。本実施形態はM P E G (Moving Picture Expert Group)に準拠したT S P (トランスポートパケット) の転送例である。

25

ENC（以下暗号化情報と記す） 9 1 0 は実データ 9 0 5 が暗号化されているか否かを示す。

図 2 は本発明の実施形態における送信装置と受信装置の関係をあらわす図である。送信装置 1 1 0 と受信装置 1 2 8 とは IEEE 1 3 9 4 バス（以下 1 3 9 4
5 バスと記す） 1 1 1 を通じてつながれている。

先ず送信装置 1 1 0 における各ブロックの機能を以下に説明する。

信号源 1 0 0 は、 1 3 9 4 バス 1 1 1 上に送信しようとする 1 8 8 バイト単位の MPEG のトランスポートパケット T S P（図示せず）を暗号化手段 1 0 1 に対して出力する。すなわち本実施形態では、信号源 1 0 0 は 1 8 8 バイトの固定
10 長のデータを出力する。暗号化手段 1 0 1 は鍵生成手段 1 0 6 から与えられる暗号鍵 1 0 9 を用いて信号源 1 0 0 から受け取った T S P を暗号化して出力する。本実施形態では暗号化鍵 1 0 9 が復号化情報に相当する。出力命令 1 0 5 は鍵生成手段 1 0 6 から暗号化手段 1 0 1 に対する命令であり、通常出力、暗号化出力および空出力の 3 種類の命令がある。出力命令 1 0 5 を受け取った暗号化手段 1
15 0 1 は、その命令の内容が通常出力である場合には、信号源 1 0 0 から受け取った T S P をそのまま出力し、暗号化情報 9 1 0 には値 0 を出力する。また出力命令 1 0 5 の内容が暗号化出力である場合には、T S P を鍵生成手段 1 0 6 から受け取った暗号鍵 1 0 9 で暗号化して出力し、暗号化情報 9 1 0 には値 1 を出力する。また出力命令 1 0 5 の内容が空出力である場合には、信号源 1 0 0 から T S
20 P を受け取るたびに空信号（図示せず）を出力するとともに、暗号化情報 9 1 0 には値 1 を出力する。ソースパケット化手段 1 0 2 は、暗号化手段 1 0 1 から受け取った 1 8 8 バイトの T S P に 4 バイトのソースパケットヘッダを付加して 1 9 2 バイトのソースパケット（実データ 9 0 5）を出力する。C I P ブロック化手段 1 0 3 は、ソースパケット化手段 1 0 2 から受け取ったソースパケットに C
25 I P ヘッダ 9 5 4 を付加してアイソクロノスペイロード 9 5 2 を出力する。その

際にCIPブロック化手段103は、暗号化手段101から受け取った暗号化情報910をCIPヘッダ954内に配置する。アイソクロノスケット化手段107はCIPブロック化手段103から受け取ったアイソクロノスペイロード952にアイソクロノスケットヘッダ900、ヘッダCRC901およびデータCRC903を付加してアイソクロノスケットを出力する。このとき、アイソクロノスペイロード952の内容がAVプロトコルに準拠したデータであるので、タグ907の値は1とする。鍵生成手段106は、後述するように受信装置128との間で、図3に示すエイシンクロナスケットのやりとりにより暗号鍵109を受信装置128に送信し、また前述のように暗号化手段101に対しても暗号鍵109を出力する。

1394パケット入出力手段108は、1394バス111と送信装置110との間でアイソクロノスケットおよびエイシンクロナスケットの入出力を行う。すなわち、1394パケット入出力手段108は、アイソクロノスケット化手段107から受け取ったアイソクロノスケットおよび鍵生成手段106から受け取ったエイシンクロナスケットを1394バス111上に出力するとともに、1394バス111から受信したエイシンクロナスケットを鍵生成手段106へと出力する。

次に受信装置128の各ブロックの機能を以下に説明する。

1394パケット入出力手段127は、1394バス111と受信装置128との間でアイソクロノスケットおよびエイシンクロナスケットの入出力を行う。すなわち、1394パケット入出力手段127は、1394バス111から受信したアイソクロノスケットをペイロード抽出手段123に対して出力し、1394バス111から受信したエイシンクロナスケットを鍵生成手段125に対して出力する。また、鍵生成手段125から受け取ったエイシンクロナスケットを1394バス111に対して出力する。

- ペイロード抽出手段123は、1394バス111から受信したアイソクロノ
スパケットを1394パケット入出力手段127から受取り、アイソクロノスパ
ケットのタグ907の値が1である場合にはアイソクロノスペイロード952の
中身がAVプロトコル準拠のデータであることを知り、アイソクロノスペイロー
ド952を実データ抽出手段122に対して出力する。実データ抽出手段122
は、受けとったアイソクロノスペイロード952に実データ905が含まれる場
合には、アイソクロノスペイロード952の先頭のCIPヘッダ954を除去し
た実データ905を復号化手段121に対して出力する。また、実データ抽出手
段122は、CIPヘッダ954から抽出したソースID906と暗号化情
報910とを鍵生成手段125に対して出力する。また暗号化情報910は、復
号化手段121に対しても同様に出力される。鍵生成手段125は、後述するよ
うに送信装置110との間でのエイシンクロナス通信によるエイシンクロナスパ
ケットのやりとりにより暗号鍵126を受け取り、復号化手段121に対して暗
号鍵126を出力する。復号化手段121は、実データ抽出手段122から受信
した暗号化情報910の値が0の時には、実データ抽出手段122から受け取っ
た実データ905を映像音声化手段120に対してそのまま出力し、暗号化情報
910の値が1の時には、鍵生成手段125から受け取った暗号鍵126を用い
て実データ905を復号化し、復号化した結果を映像音声化手段120に対して
出力する。
- 次に前述のエイシンクロナス通信によるエイシンクロナスパケット伝送につい
て説明する。

図3A～Cは、エイシンクロナス通信により伝送されるエイシンクロナスパケ
ットのフォーマットを示し、このうち図3Aおよび図3Cは、本実施形態におけ
る鍵生成手段106と鍵生成手段125との間でやりとりされるAKEコマンド
(AKE: Authentication and Key Exchange)のコマンドフォーマットであ

り、図3Bはレスポンスフォーマットである。これらのコマンドおよびレスポンスは、AV/Cコマンドセットに属するコマンドとして、エイシンクロナス通信を用いて送信装置110と受信装置128との間でやり取りされる。これらのコマンドおよびレスポンスをやりとりすることにより、送信装置110および受信装置128の間で、相手装置の認証や暗号鍵109、126のやりとりに必要な情報の交換が行われる。前記AKEコマンドには、相手装置に対する何らかの動作を要求するAKEコントロールコマンドと、相手装置の状態や能力を問い合わせるためのAKEステータスコマンドとがある。

図3AはAKEステータスコマンドのフォーマットをあらわす図である。AKEステータスコマンドにおいて、オペコード208は、当該コマンドがAKEコマンドであることを示す。アルゴリズムID200は固定値0であり、0以外の値は将来の拡張のために予約となっている。

図3BはAKEステータスコマンドに対するレスポンスのフォーマットをあらわす。図3AのAKEステータスコマンドを受け取った装置が、そのAKEステータスコマンドを発行した装置に対して返送するのがこのレスポンスである。送信装置110と受信装置128との間で、相互認証および暗号鍵109、126の伝達を行う一連の情報交換手順には複数の種類があり、アルゴリズム領域201には、当該レスポンスを返す装置が実行可能な情報交換手順の識別子がビットアサインされている。すなわち、受信装置128は、前記の手順により暗号化されたTSPを検出してから暗号鍵109、126を受け取るまでの間に、送信装置110との間で複数のコマンドおよびレスポンスをやり取りする。このコマンドおよびレスポンスをやり取りする情報交換手順には複数の種類があり、当該レスポンスを返す装置は、自身で実行可能な情報交換手順をアルゴリズム領域201における当該ビットの値を1にしてあらわす。アルゴリズム領域201のサイズは16ビットであるので、最大16種類の情報交換手順をあらわすことが可能

である。最大データ長 2 1 2 は、AKE コマンドおよびそれに対するレスポンス
をやり取りする際に、受信可能な最大データ長が何バイトであるかを示す。

図 3 C は AKE コントロールコマンドのフォーマットをあらわす。AKE コン
トロールコマンドにおけるアルゴリズム領域 2 0 1 は、アルゴリズム ID 2 0 0
5 の値が 0 である時には、実行中の情報交換手順をあらわす。アルゴリズム領域 2
0 1 の各ビットは、AKE コントロールコマンドおよび AKE コントロールコマ
ンドに対するレスポンスにおいては、必ず 1 つのビットだけが 1 で他のビットは
0 となっており、その値 1 の 1 ビットが現在実行中の情報交換手順をあらわして
いる。ラベル 2 0 2 は、複数の AKE コントロールコマンド間の対応を明確にし
10 るために用いられる。例えば、1 つの装置が他の装置に対して AKE コントロー
ルコマンドを送信したとして、その AKE コントロールコマンドを受信した装置
は、受信した AKE コントロールコマンドに呼応する別の AKE コントロールコ
マンド返送するという規定が、ある情報交換手順で定められているとする。この
場合、両 AKE コントロールコマンド間の呼応関係を明確にするために、返送す
15 る AKE コントロールコマンドに挿入されるラベル 2 0 2 は、最初に受信した A
KE コントロールコマンドに挿入されていたラベル 2 0 2 と同じ値を使用する。
ステップ番号 2 0 3 は、情報交換手順の中でやりとりされる順に、個々の AKE
コントロールコマンドに対して 1 から順に付けられるシリアル番号である。

サブファンクション 2 9 9 は、表 1 に示す値をとり、この値によってその AK
20 E コマンドの持つ意味が定まる。

表 1

サブファンクション	値
メイクレスポンス	00 ₁₆
ベリファイミー	01 ₁₆
クリエイトキーインフォ	10 ₁₆
リコンストラクトキー	11 ₁₆
エクスチェンジ	20 ₁₆

サブファンクション 299 の内容がメイクレスポンスである場合には、当該 AKE コントロールコマンドはコマンドを受信する装置に対する認証のチャレンジを意味する。このときデータ 207 には、相手の装置を認証するための乱数である認証チャレンジデータが含まれる。このコマンドを受信した装置は、サブファンクション 299 の内容をペリファイミーにした AKE コントロールコマンドを返送する。この返送の際にデータ 207 に格納されるデータは、先程受信したデータ 207 中の認証チャレンジデータに対して、あらかじめ定められた演算を行った結果である認証レスポンスデータである。この演算に使用される鍵情報は、あらかじめ正規に認定された機器にのみ付与されている鍵であるので、返送されてきた認証レスポンスデータを調べれば、演算を行った機器が正しく認定された機器であるか否かを認証することができる。

サブファンクション 299 の内容がクリエイトキーインフォである場合には、当該 AKE コントロールコマンドは、このコマンドを受信する装置に対する暗号鍵 109 の要求を意味する。この AKE コントロールコマンドを受け取った装置は、サブファンクション 299 の内容がリコンストラクトキーである AKE コントロールコマンドを返送する。この時、データ 207 には暗号化された暗号鍵 109 が格納されて返送される。

サブファンクション 299 の内容がエクスチェンジである場合には、当該 AKE コントロールコマンドは、コマンドを送信する機器と受信する機器との間での鍵情報の交換を意味する。この鍵情報はデータ 207 に格納されて転送され、機器間の間接認証や、機器共有鍵の作成のために使用される。

表 1 に挙げられている以外のサブファンクションの値は将来における拡張のための予約となっている。チャンネル番号 204 は、送信装置 110 と受信装置 128 との間で行うアイソクロノス通信のチャンネルの番号を示す。このチャンネル番号

204は、サブファンクション299の内容がクリエイトキーインフォまたはリ
コンストラクトキーの時にのみ有効であり、それ以外の場合にはこの値は16進
表記でFFとなる。ブロック番号205および総ブロック番号206は、AKE
コントロールコマンドでやり取りすべきデータが一つのAKEコマンドで伝送し
5 きれない場合に使用する。すなわちこの場合には、当該データはいくつかのブロ
ックに分割され、複数回に分けて転送される。総ブロック番号206は当該デー
タを分割したブロック個数をあらわし、ブロック番号205は、データ207が
幾つ目のブロックのデータであるかを示す。データ長209はデータ207に含
まれる有効なデータ長をバイト数で表す。データ207はAKEコントロールコ
10 マンドによってやり取りされるデータである。AKEコントロールコマンドを受
信した装置はそのAKEコントロールコマンドに対する応答を返す。その際の応
答のフォーマットおよび値は、受け取ったAKEコントロールコマンドのフォー
マットおよび値と同じであるが、応答にはデータ207が含まれない点だけが唯
一異なる。

15 図4は、送信装置110から受信装置128に対して暗号鍵109、126が
送信されるまでの間に、両装置間でやり取りされるAV/Cコマンドの具体例を
時系列で模式的にあらわした図である。まず、図4に示すAV/Cコマンドのや
り取りが始まるまでの両装置の動作を簡単に説明する。

まず初期状態として、暗号化されていないTSPが送信装置110から送信さ
20 れている状況を想定する。信号源100から出力されるTSPが暗号化手段10
1に入力される。暗号化手段101は、出力命令105の内容が通常出力である
ので、TSPを暗号化せずにそのままソースパケット化手段102へ出力すると
ともに、暗号化情報910には値0を出力する。ソースパケット化手段102は、
受け取ったTSPに4バイトのソースパケットヘッダを付加して、CIPブロ
25 ック化手段103へ出力する。CIPブロック手段103は、これに8バイトのC

I P ヘッダ 9 5 4 を付加し、アイソクロノス₂パケット化手段 1 0 7 に対して、アイソクロノス₁ペイロード 9 5 2 として出力する。この際、C I P ヘッダ 9 5 4 に含まれる暗号化情報 9 1 0 には、暗号化手段 1 0 1 から入力した値である 0 をそのまま格納する。アイソクロノスパケット化手段 1 0 7 は、受け取ったアイソクロノス₁ペイロード 9 5 2 に、アイソクロノスパケットヘッダ 9 0 0、ヘッダ C R C 9 0 1 およびデータ C R C 9 0 3 を付加して、アイソクロノスパケットを作成する。このアイソクロノスパケットは、1 3 9 4 パケット入出力手段 1 0 8 によって 1 3 9 4 バス 1 1 1 上へ出力される。この際、当該アイソクロノスパケットが A V プロトコル準拠のアイソクロノスパケットであるので、アイソクロノスパケットヘッダ 9 0 0 に含まれるタグ 9 0 7 の値は 1 となる。

信号源 1 0 0 から出力される T S P が変化した時、すなわち著作権で保護されていない映像音声情報から著作権で保護されている映像音声情報へと切り替わった時、この変化を検出した鍵生成手段 1 0 6 は、出力命令 1 0 5 を通常出力から空出力へと変化させるとともに、T S P を暗号化するための暗号鍵 1 0 9 を暗号化手段 1 0 1 に渡す。

出力命令 1 0 5 の内容が空出力であるとき、暗号化手段 1 0 1 は、信号源 1 0 0 から T S P を受け取るたびにソースパケット化手段 1 0 2 に対して空信号を出力するとともに暗号化情報 9 1 0 に値 1 を出力する。暗号化手段 1 0 1 から空信号を受け取ったソースパケット化手段 1 0 2 は、ソースパケットヘッダを付加せず、受け取った空信号をそのまま C I P ブロック化手段 1 0 3 へと伝達する。C I P ブロック化手段 1 0 3 は空信号を受け取ると、C I P ヘッダ 9 5 4 だけをアイソクロノスパケット化手段 1 0 7 へ出力する。この時、C I P ヘッダ 9 5 4 中の暗号化情報 9 1 0 は、暗号化手段 1 0 1 が出力した値 1 をそのまま用いる。アイソクロノスパケット化手段 1 0 7 は、C I P ブロック化手段 1 0 3 から受け取った C I P ヘッダ 9 5 4 をアイソクロノス₁ペイロード 9 5 2 としてアイソクロ

ノス packets を作成し、1394 packets 入出力手段 108 へ出力する。この際、当該アイソクロノス packets は AV プロトコルに準拠しているので、タグ 907 の値は 1 となる。1394 packets 入出力手段 108 は受け取ったアイソクロノス packets を 1394 バス 111 上へ出力する。当該アイソクロノス packets は

5 継続的に出力され、1394 バス 111 上には CIP ヘッダ 954 のみをアイソクロノス ペイロード 952 に含んだアイソクロノス packets が継続的に流れるようになる。このアイソクロノス packets を受信した受信装置 128 では、1394 packets 入出力手段 127 がタグ 907 を調べ、AV プロトコルに準拠したアイソクロノス packets であることを検出した後、当該アイソクロノス packets を

10 ペイロード抽出手段 123 へ出力する。ペイロード抽出手段 123 は受け取ったアイソクロノス packets からアイソクロノス ペイロード 952 を抽出して実データ抽出手段 122 へ出力する。実データ抽出手段 122 は、CIP ヘッダ 954 に含まれる暗号化情報 910 とソース ID 906 とを鍵生成手段 125 へ出力する。鍵生成手段 125 は、暗号化情報 910 を調べて値が 1 であることを検出したのち、ソース ID 906 から当該アイソクロノス packets を出力しているのが

15 出力装置 110 であることを知る。しかる後、鍵生成手段 125 は AV/C コマンドを用いて暗号鍵 109、126 を要求する過程、すなわち図 4 に示した過程へと移る。

図 4 において、先ず AKE ステータス コマンド 300 が受信装置 128 から送信装置 110 へ送信される。これにより受信装置 128 は、送信装置 110 が実行可能な情報交換手順を問い合わせることになる。これに応じて送信装置 110 は AKE レスポンス 301 を受信装置 128 に対して返送する。この AKE レスポンス 301 には、送信装置 110 が実行可能な情報交換手順が、アルゴリズム領域 201 内にビットアサインされており、これによって受信装置 128 は、送信装置 110 がどの情報交換手順を実行可能なのかを知ることができる。具体例

20

25

としては、送信装置 1 1 0 が実行可能な情報交換手順が第 2 番目のものと第 6 番目のものの 2 つであった場合には、AKE レスポンス 3 0 1 内のアルゴリズム領域 2 0 1 は 2 進表記で 00000000000100010 となる。

5 AKE レスポンス 3 0 1 を受信した受信装置 1 2 8 は、送信装置 1 1 0 が実行可能でかつ受信装置 1 2 8 自身も実行可能な情報交換手順の中から、最適な 1 つの手順を選択し、以降その手順にしたがって AV/C コマンドをやりとりする。

いま仮に受信装置 1 2 8 の側で、実行可能な情報交換手順が第 2 番目のものと第 8 番目のものであった場合には、送信装置 1 1 0 および受信装置 1 2 8 の双方で実行可能な情報交換手順は、第 2 番目のものだけということになり、以降は第 2

10 番目の手順を用いて認証および情報の交換が行われることになる。この手順に含まれる AKE コントロールコマンドでは、アルゴリズム ID の値が 0 で、アルゴリズム領域 2 0 1 の値が 1 6 進表記で 00000000000000010 となる。情報交換手順で指定される手順には、各種 AKE コントロールコマンドのやり取りの順番だけでなく、各 AKE コントロールコマンドで送られるデータ 2 0 7 のフォーマットや処理方法も規定されている。

15

第 2 番目の情報交換手順に従い、鍵生成手段 1 2 5 はメイクレスポンスコマンド 3 0 2 を送信装置 1 1 0 に対して送信する。このメイクレスポンスコマンド 3 0 2 中のデータ 2 0 7 には、鍵生成手段 1 2 5 で発生させた 2 つの乱数、RR a と RR b とが暗号化されて含まれているとともに、アルゴリズム領域 2 0 1 には第 2 番目の手順をあらわす識別情報が含まれている。この暗号化に際して使用する鍵は、正規に認められた送信装置と受信装置とにあらかじめ与えられている共通の秘密鍵である。メイクレスポンスコマンド 3 0 2 を受け取った鍵生成手段 1 0 6 は、受け取ったメイクレスポンスコマンド 3 0 2 のアルゴリズム領域 2 0 1 を調べて、以降は第 2 番目の手順を用いて認証および情報の交換を行うことを

20

25 知る。鍵生成手段 1 0 6 は、第 2 番目の手順を実行可能なのであるから、第 2 番

目の手順に基づいて送信されてくるメイクレスポンスコマンド302のデータ207にはこの秘密鍵で暗号化された2つの乱数が含まれていることを知っている。そこで鍵生成手段106は、この秘密鍵を用いてデータ207からRRaおよびRRbの2つの乱数を取り出したのち、レスポンスを作成することが可能であることを示す応答303を返す。しかるのち鍵生成手段106は、取り出した乱数のうちの一つであるRRaをデータ207に格納して、ベリファイミーコマンド304を受信装置128に対して送信する。これが先程のメイクレスポンスコマンド302にて要求されたレスポンスである。このベリファイミーコマンド304を含め、これ以降、送信装置110と受信装置128との間でやり取りされる各AKEコマンドのアルゴリズム領域201には全て、2番目の手順をあらわす識別情報が含まれる。

ベリファイミーコマンド304を受信した鍵生成手段125は、データ207の内容であるRRaが、自分が先程発生させた乱数RRaと一致することを確認したのち、ベリファイミーコマンド304に対して、正常にベリファイしたことを示す応答305を返す。これにより、鍵生成手段125は、送信装置110が正規に認められた送信装置であると認証する。

次に送信装置110は、前記メイクレスポンス302以降と同じ手順によって、メイクレスポンスコマンド306およびベリファイミーコマンド308を用いて、受信装置128が正規に認められた受信装置であることを確認する。但しこの際に使用される乱数はRTaおよびRTbであり、ベリファイミーコマンド308で送り返される乱数はRTbである。

この時点で送信装置110および受信装置128の双方は、乱数RRbと乱数RTbとがともにわかっていることになり、また、お互いが正規に認められた装置であることを確認したことになる。鍵生成手段106と鍵生成手段125とは、それぞれ別個に、2番目の手順で定められている共通の演算方法により、RRb

とRTbとから一時鍵（図示せず）を生成する。この一時鍵は、送信装置110および受信装置128の両装置のみが共有する共通の鍵である。

次に鍵生成手段125はクリエイトキーインフォコマンド310を送信装置110に対して送信する。この際、クリエイトキーインフォコマンド310のチャンネル番号204には、現在受信装置128が受信中のアイソクロノスパケットのチャンネル番号が格納される。このクリエイトキーインフォコマンド310を受け取った鍵生成手段106は、TSPの暗号化に用いる暗号鍵109を前記の一時鍵で暗号化したのち、クリエイトキーインフォコマンド310が正常に完了したことを示す応答311を返送する。続いて、鍵生成手段106は、この暗号鍵109を一時鍵で暗号化した結果をデータ207に格納したりリコンストラクトキーコマンド312を受信装置128へ送る。鍵生成手段125は一時鍵を用いて、受け取ったりリコンストラクトキーコマンド312のデータ207を復号化し、その結果暗号鍵126を得たのち、リコンストラクトキーコマンド312を正常に完了したことをあらわす応答313を返す。暗号鍵109と暗号鍵126とは、
10 09を一時鍵で暗号化した結果をデータ207に格納したりリコンストラクトキーコマンド312を受信装置128へ送る。鍵生成手段125は一時鍵を用いて、受け取ったりリコンストラクトキーコマンド312のデータ207を復号化し、その結果暗号鍵126を得たのち、リコンストラクトキーコマンド312を正常に完了したことをあらわす応答313を返す。暗号鍵109と暗号鍵126とは、
15 同じ一時鍵を用いて暗号化と復号化を行ったので、同じ鍵である。この暗号鍵126は鍵生成手段125から復号化手段121に対して出力される。以上の手順で復号化情報の付与が完了する。

リコンストラクトキーコマンド312を送信した鍵生成手段106は、暗号化手段101に対して暗号化出力を示す出力命令105を出力する。これを受けた
20 暗号化手段101は、信号源100から受け取るTSPを暗号鍵109で暗号化し、ソースパケット化手段102への出力を開始する。これにより、1394バス111上に、暗号鍵109にて暗号化されたTSPをアイソクロノスペイロード952に含むアイソクロノスパケットが送信装置110から送信されるようになる。受信装置128で受信された当該アイソクロノスパケットは、前述したように、復号化手段121において暗号鍵126を用いて復号化され、映像音声化
25 うに、復号化手段121において暗号鍵126を用いて復号化され、映像音声化

手段120へ出力される。

前記一連のAKEコントロールコマンドにおいて、メイクレスポンスコマンド302とベリファイミーコマンド304、メイクレスポンスコマンド306とベリファイミーコマンド308、およびクリエイトキーインフォコマンド310と
5 リコンストラクトキーコマンド312はそれぞれ同じラベル202を持つ。また、メイクレスポンスコマンド302、ベリファイミーコマンド304、メイクレスポンスコマンド306、ベリファイミーコマンド308、クリエイトキーインフォコマンド310およびリコンストラクトキーコマンド312はそれぞれ1、2、3、4、5、6なる値をステップ番号203に持つ。

10 送信装置110の出力するアイソクロノスケットに含まれる実データ部105が、暗号化された実データ105から暗号化されない実データ105へと変化した場合には、復号化手段121は、暗号化情報910の変化を検出して復号化をやめ、実データ抽出手段122から受け取った出力をそのまま映像音声化手段120へと渡すようになる。

15 また、前記の図4に示した過程が始まった後に、1394バス111にバスリセットが発生した場合には、メイクレスポンスコマンド302以降の手順を最初からやりなおす。

以上のように本実施形態によれば、アイソクロノスケット内の実データの暗号化状況を示す暗号化情報が実データと一緒に送信装置から送信されることにより、アイソクロノスケットを受信した受信装置は、アイソクロノスケット内に
20 含まれる暗号化情報を調べ、実データが暗号化されていることを検出すると、送信装置に対して実データを復号するための暗号鍵を要求し、要求を受けた送信装置はその受信装置に対して暗号鍵を付与するので、送信装置が受信装置に復号のための暗号鍵を付与する際の手順が極めて簡素なデータ転送方法を実現できる。

25 また以上のように本実施形態によれば、アイソクロノス通信で転送されるアイ

ソクロノスケットには、実データの暗号化状況を示す暗号化情報と実データとが含まれ、暗号化は実データに対してのみ行ってデータ転送を行うことにより、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が、暗号化された実データを受信しても誤動作する可能性のないデータ転送方法を実現できる。

- 5 また以上のように本実施形態によれば、送信装置の送信している同期データを受信装置が継続的に受信している最中に、同期データの暗号化が始まったとしても、C I Pヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できる。

- 10 なお、本実施形態においては、暗号鍵による暗号化が一旦開始されれば、全ての転送単位に含まれる実データは暗号化されて送信されるが、全ての転送単位に対して暗号化を行う必要はない。例えば暗号化された転送単位と暗号化されない転送単位とが交互に送信されても、C I Pヘッダ中に暗号化情報が含まれているので、受信装置においては復号を正常に行うことが可能であり、同様の効果を得ることが可能である。更にこの場合、暗号化を行う転送単位の割合を受信装置が
- 15 送信装置に指定しても、得られる効果が変わらないことは言うまでもない。但し、M P E Gのソースパケットはその大きさが192バイトであるが、M E P Gの高データレート転送（12Mbps以上）を行う際には複数のソースパケットが一つのアイソクロノスペイロードに格納される。このとき、同一のアイソクロノスペイロードの中に、暗号化されたソースパケットと暗号化されないソースパケット
- 20 との両方があってはならないことも言うまでもない。

- 25 なお、本実施形態においては、暗号鍵による暗号化は実データ部全てに対して行われたが、全ての部分に暗号化を行う必要はない。例えば、実データ部の前半分だけを暗号化したり、実データ部を4等分したうちの最初と3番目の2個所を暗号化して送信しても同様の効果が得られる。この場合は、暗号化を行った場所
- 25 や割合を示す情報をC I Pヘッダに挿入して送信すれば、受信装置側で適切な復

号化を行うことが可能である。更に、C I Pヘッダには、実データが暗号化されているか否かを示す暗号化情報のみを挿入しておき、C I Pヘッダを見て暗号化されていることを検出した受信装置が、実データ部のどの部分がどのくらい暗号化されているかという情報を、エイシクロナス通信によって送信装置に問い合わせ

5 わせても、同様の効果を得ることが可能である。この場合、暗号化を行う場所や割合を、受信装置が送信装置に対してエイシクロナス通信を用いて指定しても、同様の効果が得られることは言うまでもない。また、実データ部の中でデータの重要性が高い部分についてのみ暗号化を行うと、暗号化および復号化にかかる負荷が低くなり、しかも十分な暗号化の効果が得られることも言うまでもない。

10 なお、本実施形態においては、送信装置と受信装置との間で相互の認証が完了するまでは実データを含まないC I Pヘッダのみのアイソクロノスパケットを転送したが、C I Pヘッダのみのアイソクロノスパケットを出力することなく、最初から暗号化された実データを含むアイソクロノスパケットを出力しても、同様の効果が得られることは言うまでもない。

15 なお、本実施形態においては、送信装置と受信装置の間でやりとりされるAKEコントロールコマンドの転送手順を相互の調停により決定したが、受信装置が実行可能な手順が一つだけに限られる場合にはこの調停手順をおこなわず、受信装置が実行可能な唯一の手順でコマンドの転送を開始しても同様の効果が得られることは言うまでもない。この場合には、全ての正規に認証された機器が最低限

20 実行可能な基本手順を定めておくことが望ましい。

なお、本実施形態においては、送信装置と受信装置との間で直接認証を行い、秘密鍵による復号化情報の伝送を行ったが、認証および復号化情報の伝達手段はこれに限らない。例えば公開鍵を用いて相互に間接認証および一時鍵の作成を行ない、一時鍵を用いて復号化情報の伝送を行っても構わない。以下、その手順を

25 簡単に説明する。

送信装置および受信装置は、相互の調停で定めた手順により、相互の間接認証に必要となる鍵情報をAKEコントロールコマンドのデータ207に格納して送信しあう。このとき、サブファンクション299はエクスチェンジをあらわす。

これにより、送信装置と受信装置は、互いに正規に認証された機器であれば同じ

- 5 一時鍵を共有することになるので、それ以降は本実施形態と同様の手順で、クリエイトキーインフォコマンドおよびリコンストラクトキーコマンドを用いて復号化情報の伝送を行うことが可能となる。

- 10 なお、本実施形態においては、送信装置と受信装置の間でやりとりされるAKEコントロールコマンドの転送手順は相互の調停により決定されたが、送信装置で実行可能な手順の種類があらかじめわかっている場合には、この調停手順をおこなわずに、送信装置の実行可能な手順で受信装置がコマンドの転送を開始しても、同様の効果が得られることは言うまでもない。

- 15 なお、本実施形態においては、送信装置と受信装置の間でやりとりされるAKEコントロールコマンドの転送手順を相互の調停により決定したが、転送手順を決定する手段はこれに限らない。すなわち、複数の転送手順の個々について、あらかじめ定められた優先順位がある場合は、受信装置は、自身が実行可能な手順の中で最も優先順位の高い手順を用いて転送を開始し、送信装置がその手順を実行不能な時には、優先順位にしたがって順次次の手順を選択して転送を開始し、送信装置と受信装置の双方が実行可能な手順が見つかったならば、その手順を用いてAKEコントロールコマンドの転送を行っても、同様の効果が得られることは言うまでもない。

- 20 なお、本実施形態においては、送信装置が実データ部の復号に用いる復号化情報を暗号化して、受信装置へ転送したが、受信装置が復号化情報を取得するための手段はこれに限らない。すなわち、送信装置が暗号化した復号化情報を転送するのではなく、受信装置が復号化情報を取得するのに十分な情報を送信装置が受

信装置に転送し、受信装置がこの情報から間接的に復号化情報を取得してもよい。具体的には、送信装置から受信装置へはハッシュ関数の種だけが転送され、受信装置側では受信した種をもとにハッシュ関数を用いて復号化情報を取得しても同様の効果が得られることは言うまでもない。

- 5 なお、本実施形態においては、AKEコマンドのフォーマットの一例を示したが、AKEコマンドのフォーマットはこれに限らない。すなわち、本実施形態で示したAKEコマンドのフォーマットは、本実施形態を実現するための一例にすぎず、これとは異なるフォーマットのコマンドを用いても同様の効果を得ることができることは言うまでもない。

10

産業上の利用の可能性

以上のように、本発明のデータ転送方法では、同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データ部と一緒に送信されるデータ転送が行われることにより、同期データを受信した受信装置は、同期データ内に含まれる暗号識別情報を調べ、実データ部が暗号化されていることを検出すると、送信装置
15 に対して実データ部を復号するための復号化情報を要求し、この要求を受けた送信装置は受信装置に対して復号化情報を付与するので、送信装置が受信装置に復号のための鍵情報を付与する際の手順が極めて簡素なデータ転送方法を実現できるという優れた効果がある。

- 20 また以上のように本発明のデータ転送方法では、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行ってデータ転送を行うことにより、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が暗号化された同期データを受信しても誤動作する可能性の無いデータ転送方法を実現できるという優
25 れた効果がある。

また以上のように本発明のデータ転送方法では、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行ってデータ転送を行うことにより、送信装置の送信している同期データを受信装置が継続的に受信している最中に同期データの暗号化が始まったとしても、CIPヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できるという優れた効果がある。

また以上のように本発明のデータ転送方法では、送信装置と受信装置の間でやり取りされる認証情報および復号化情報の授受手順を送信装置と受信装置との間の調停によって選択することにより、将来の拡張性に優れた認証および復号化情報の授受手順を実現することが可能となる。すなわち、将来新しい認証方法や復号化情報が利用可能になった際に、新しい手順を使用できる機器と古い手順しか使用できない機器とが混在しても、新しい機器が古い手順を使用可能であれば、両機器間の調停により最適な手順を選択することが可能になる。すなわち本発明のデータ転送方法では、新しい機器と古い機器とが混在する環境においても、常に最適な手順を選択して実行可能になるという優れた効果がある。

また以上のように本発明のデータ転送方法では、暗号化された実データと暗号化されない実データとの割合を変化させることが可能であるので、暗号化された実データを復号するための高速処理が出来る専用ハードウェアを持たない受信装置でも、ソフトウェアによって復号化が可能になる。すなわち、パソコンのように復号用のハードウェアを持たない機器が受信装置である場合にも、暗号化される実データの割合を低下させ復号化処理を少なくすることにより、処理速度が遅いソフトウェアによる復号が可能になるという優れた効果がある。

また以上のように本発明のデータ転送方法では、送信装置と受信装置が相互に正規の機器であることを認証するまでの間は、実データを含まないアイソクロノ

スパケットを出力するので、限られたバスの転送帯域を無駄に使用することがなく、また正規に認証されていない機器が実データを受信してしまう可能性が非常に少なくなるという優れた効果がある。

請 求 の 範 囲

1. バス上の任意の機器が同期データを受信する同期 (isochronousアイソクロノス) 通信と、非同期データを受信する機器が特定される非同期 (asynchronousエイシンクロナス) 通信とが使用されるバスシステムにおいて、
- 5 前記同期データは実データ部を含む場合があり、前記実データ部の暗号化状況を示す暗号識別情報が前記実データ部以外の前記同期データ中に含まれており、前記同期データを受信した受信装置は、前記実データ部が暗号化されていることを前記暗号識別情報が示している場合には、前記同期データを送信している送信装置に対して、前記非同期通信を用いて前記実データ部の復号化情報を要求し、前記要求を受けた前記送信装置は、前記非同期通信を用いて前記受信装置に対して前記実データ部の前記復号化情報を暗号化した復号化情報、もしくは前記復号化情報を取得するのに必要な復号化情報取得データを送信し、前記受信装置は、前記暗号化された復号化情報を受信した場合には、前記暗号化された復号化情報から前記復号化情報を取り出し、また、前記受信装置が前記復号化情報取得データを受信した場合には、前記復号化情報取得データを用いて前記復号化情報を取得し、このようにして得られた前記復号化情報を用いて暗号化された実データ部を復号することを特徴とするデータ転送方法。
- 10
2. 前記同期データを受信した前記受信装置が、前記実データ部が暗号化されていることを検出してから前記復号化情報を取得するまでの一連の手順には、複数の種類が存在し、前記受信装置は、前記復号化情報の要求に先立って、前記送信装置が実行可能な手順の種類を前記送信装置に問い合わせ、前記受信装置は、自身と前記送信装置との双方が前記実行可能な手順の中から実行する手順を選択し、前記受信装置は選択した前記手順に基づいて前記復号化情報を取得すること特徴とする請求項 1 記載のデータ転送方法。
- 15
- 20
- 25

3. 前記送信装置と前記受信装置との双方が前記実行可能な手順が複数存在する場合には、あらかじめ定められた優先順位に従って前記手順を選択すること特徴とする請求項2記載のデータ転送方法。

4. 前記同期データを受信した前記受信装置が、前記実データ部が暗号化されていることを検出してから前記復号化情報を取得するまでの前記一連の手順には、複数の種類が存在し、前記受信装置は、前記複数の種類の手順の中からあらかじめ定められた優先順位に従って前記手順を選択して前記手順を開始し、前記受信装置の選択した前記手順を前記送信装置が実行不能である場合には、前記受信装置は、前記送信装置が実行可能な前記手順が見つかるまで、前記手順を順次選択し直して前記手順を開始し、前記受信装置は、実行可能な手順が見つかった時に、その選択した手順に基づいて前記復号化情報を取得すること特徴とする請求項1記載のデータ転送方法。

5. 前記選択された手順に基づいて、前記送信装置と前記受信装置との間で授受される前記非同期データには、実行中の前記手順の種類をあらわす識別子が含まれることを特徴とする請求項2～4のいずれか記載のデータ転送方法。

6. 前記受信装置は、前記復号化情報の要求を行う前に、前記送信装置が正規の送信装置であることを確認することを特徴とする請求項1～5のいずれか記載のデータ転送方法。

7. 前記送信装置は、前記復号化情報の要求を受けた後、受信装置が前記正規の受信装置であることを確認してから、前記実データ部の復号化情報を暗号化して送信することを特徴とする請求項1～5のいずれか記載のデータ転送方法。

8. 前記送信装置と前記受信装置とが、互いに、相手が前記正規の受信装置または前記正規の送信装置であることを確認してから、前記受信装置が前記復号化情報の要求を行うことを特徴とする請求項1～5のいずれか記載のデータ転送方法。

9. 前記受信装置が前記復号化情報を要求する前に、前記受信装置から前記送信

装置に対して、前記送信装置が共通鍵を作成するのに少なくとも必要な情報の送信と、前記送信装置から前記受信装置に対して、前記受信装置が前記共通鍵を作成するのに少なくとも必要な情報の送信とが行われ、前記送信装置は前記共通鍵を用いて前記復号化情報を暗号化して送信し、前記受信装置は受信した前記暗号化された複合化情報から前記共通鍵を用いて前記復号化情報を取り出すことを特徴とする請求項 1 ～ 8 のいずれか記載のデータ転送方法。

10. 前記暗号化は前記実データ部に対してのみ行うことを特徴とする請求項 1 ～ 5 のいずれか記載のデータ転送方法。

11. 前記送信装置は内部に実データの信号源を有し、前記送信装置は前記信号源から出力された固定長単位の前記実データ毎に暗号化の有無を決定し、暗号化された前記実データと暗号化されていない前記実データとを互いに異なる前記同期通信の出力単位内に配置して前記バスシステムへ出力することを特徴とする請求項 1 ～ 5 のいずれか記載のデータ転送方法。

12. 前記暗号化された実データと前記暗号化されていない実データとの比率を、前記受信装置が前記送信装置に対して前記非同期通信を用いて指定し、前記送信装置は前記指定に従って暗号化の有無の比率を変更することを特徴とする請求項 11 記載のデータ転送方法。

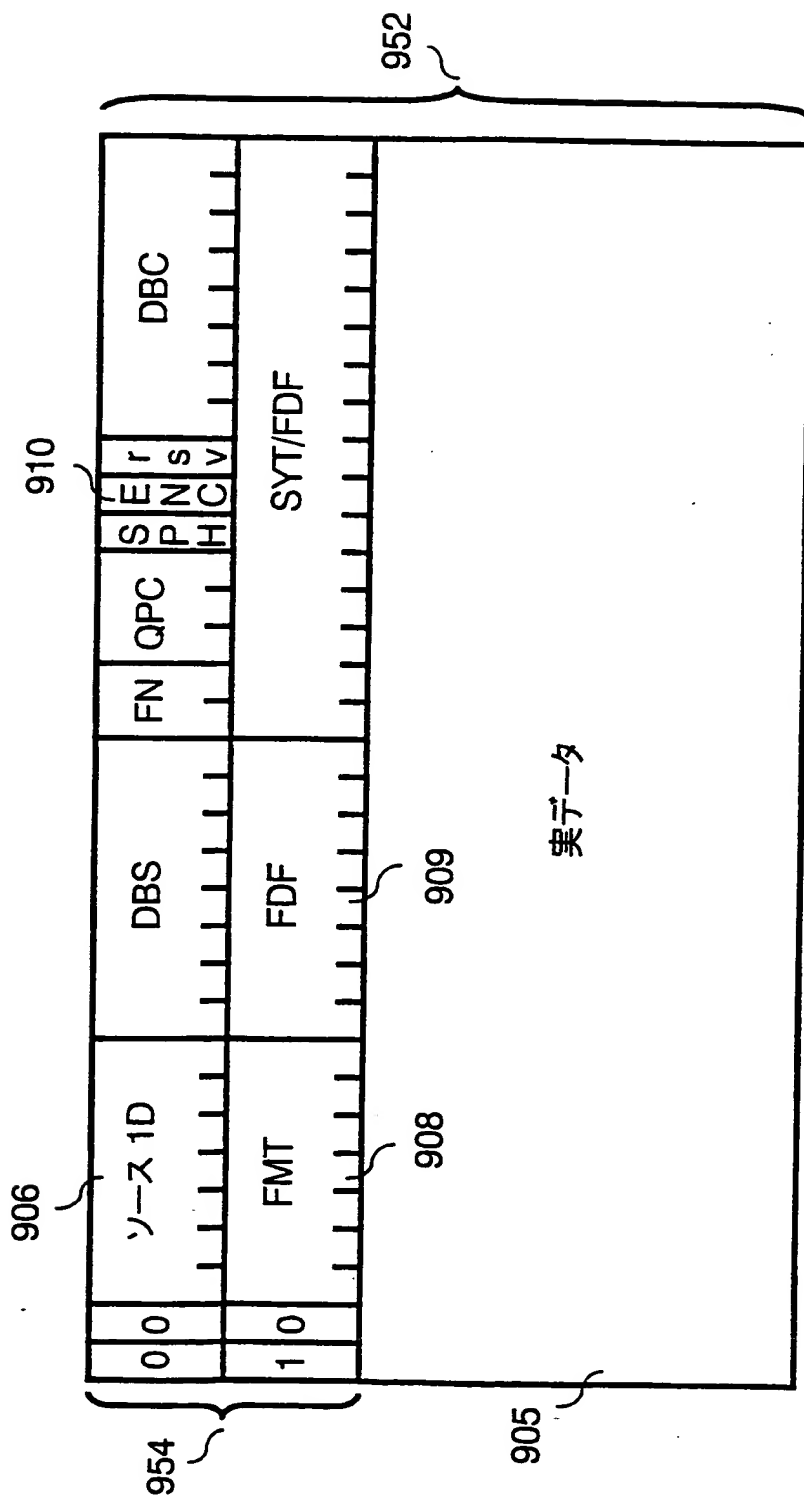
13. 前記送信装置は内部に前記実データの信号源を有し、前記送信装置は前記信号源から出力された前記固定長単位の実データについて、前記固定長単位の実データ中での前記暗号化を行う割合を決定し、前記実データを前記同期通信の出力単位内に配置して前記バスシステムへ出力することを特徴とする請求項 1 ～ 5 のいずれか記載のデータ転送方法。

14. 前記受信装置は前記送信装置に対して、前記暗号化を行う割合の指定を前記非同期通信によって行い、前記送信装置は前記指定に従って前記暗号化する割合を変更することを特徴とする請求項 13 記載のデータ転送方法。

15. 前記送信装置が前記同期データを送信する際に、少なくとも前記復号化情報を要求されるまでの間は前記同期データに前記実データ部を含めずに送信し、少なくとも前記復号化情報の要求を受け取った後に前記実データ部を含んだ前記同期データの送信を開始することを特徴とする請求項1～5のいずれか記載のデータ転送方法。

5

THIS PAGE BLANK (USPTO)



1
X

3 PAGE BLANK (USPTO)

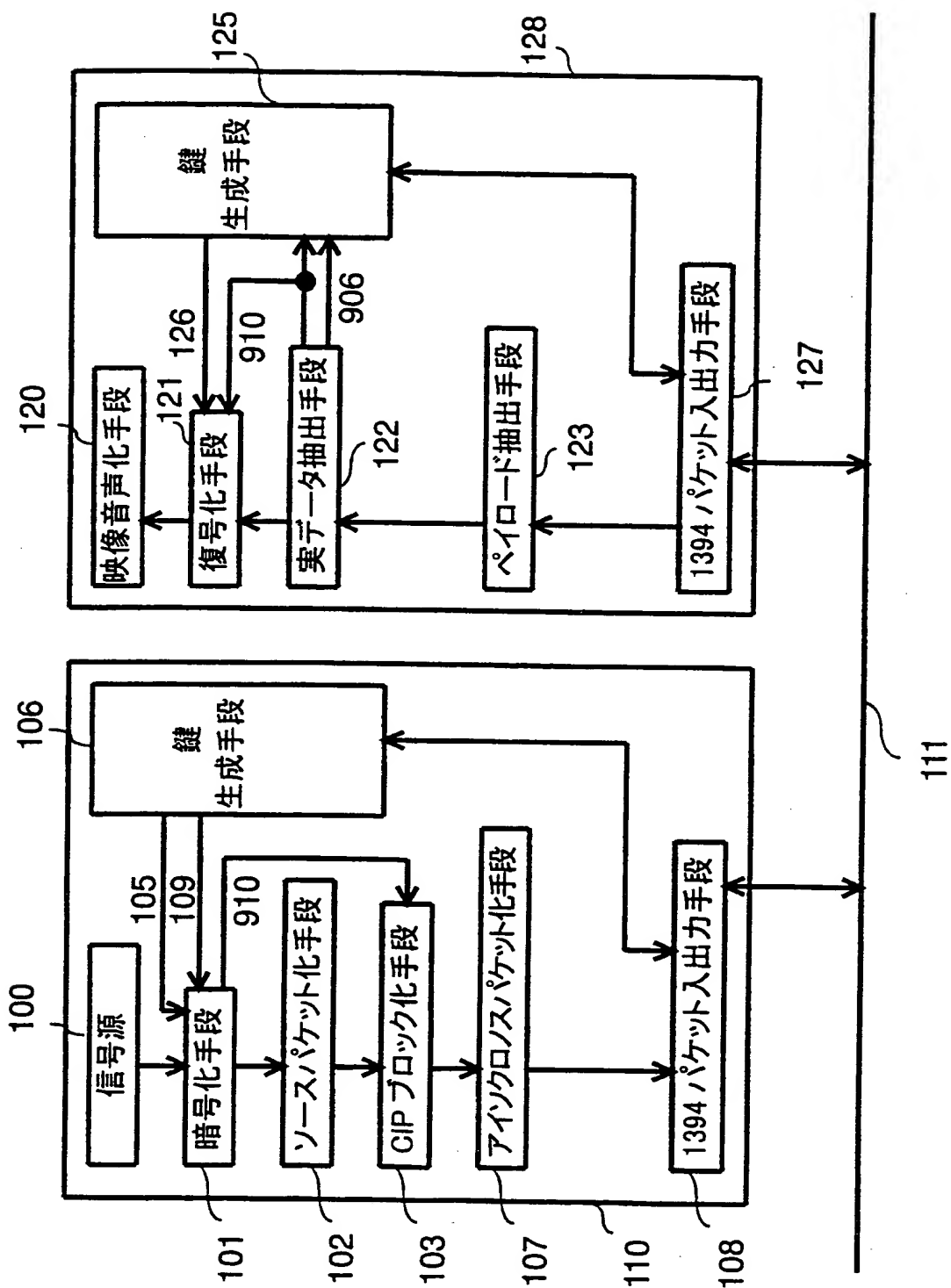


図 2

BLANK (USPTO)

3/7

図 3 A

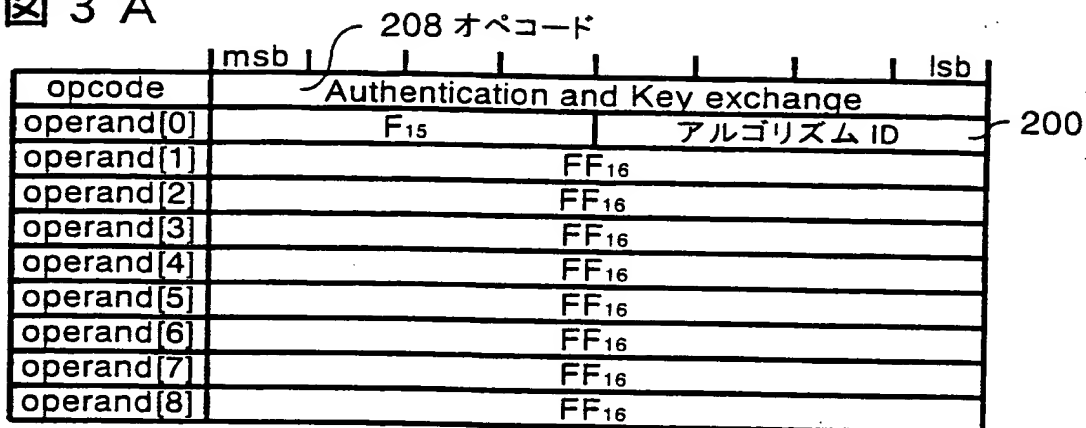


図 3 B

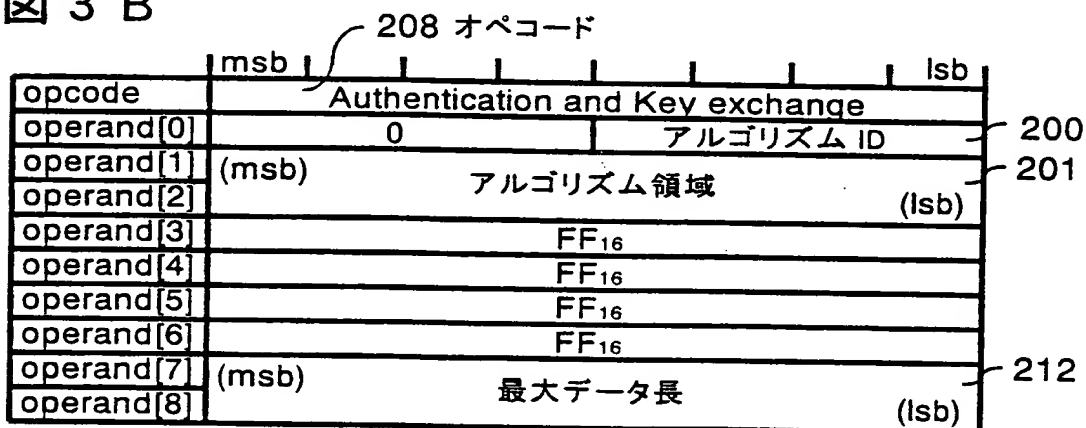
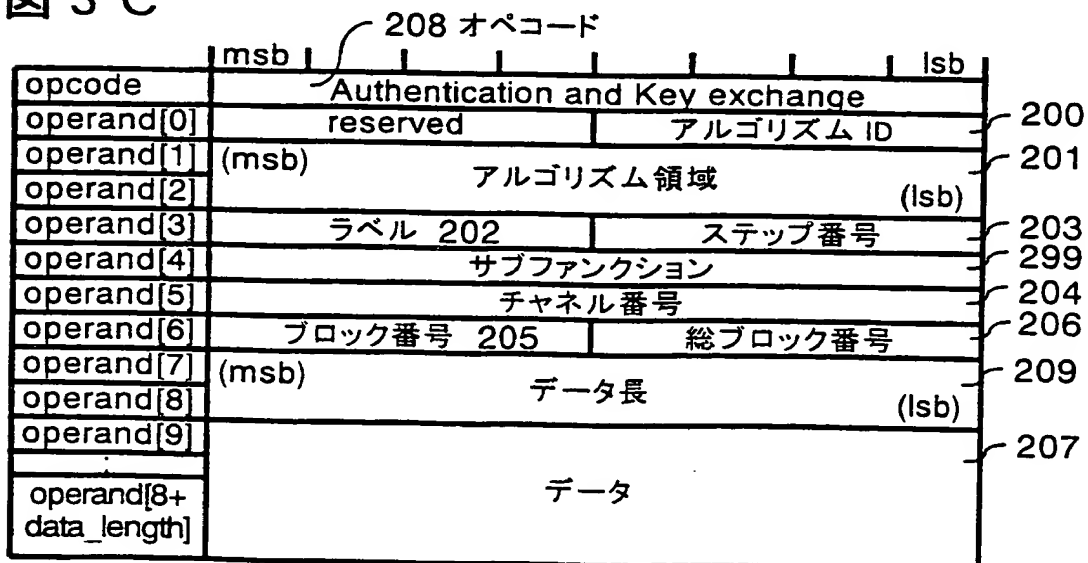


図 3 C



THIS PAGE BLANK (USPTO)

4/7

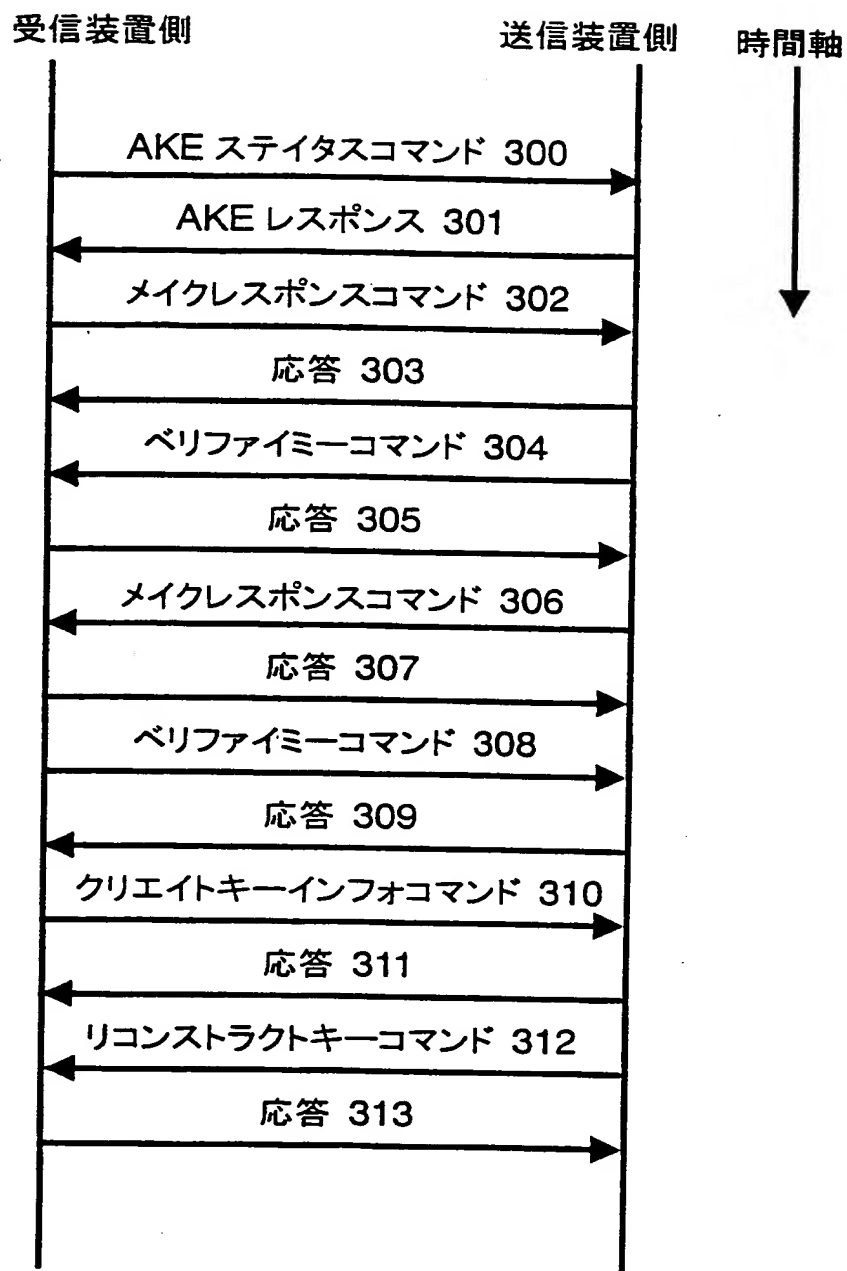


図 4

THIS PAGE BLANK (USPTO)

5/7

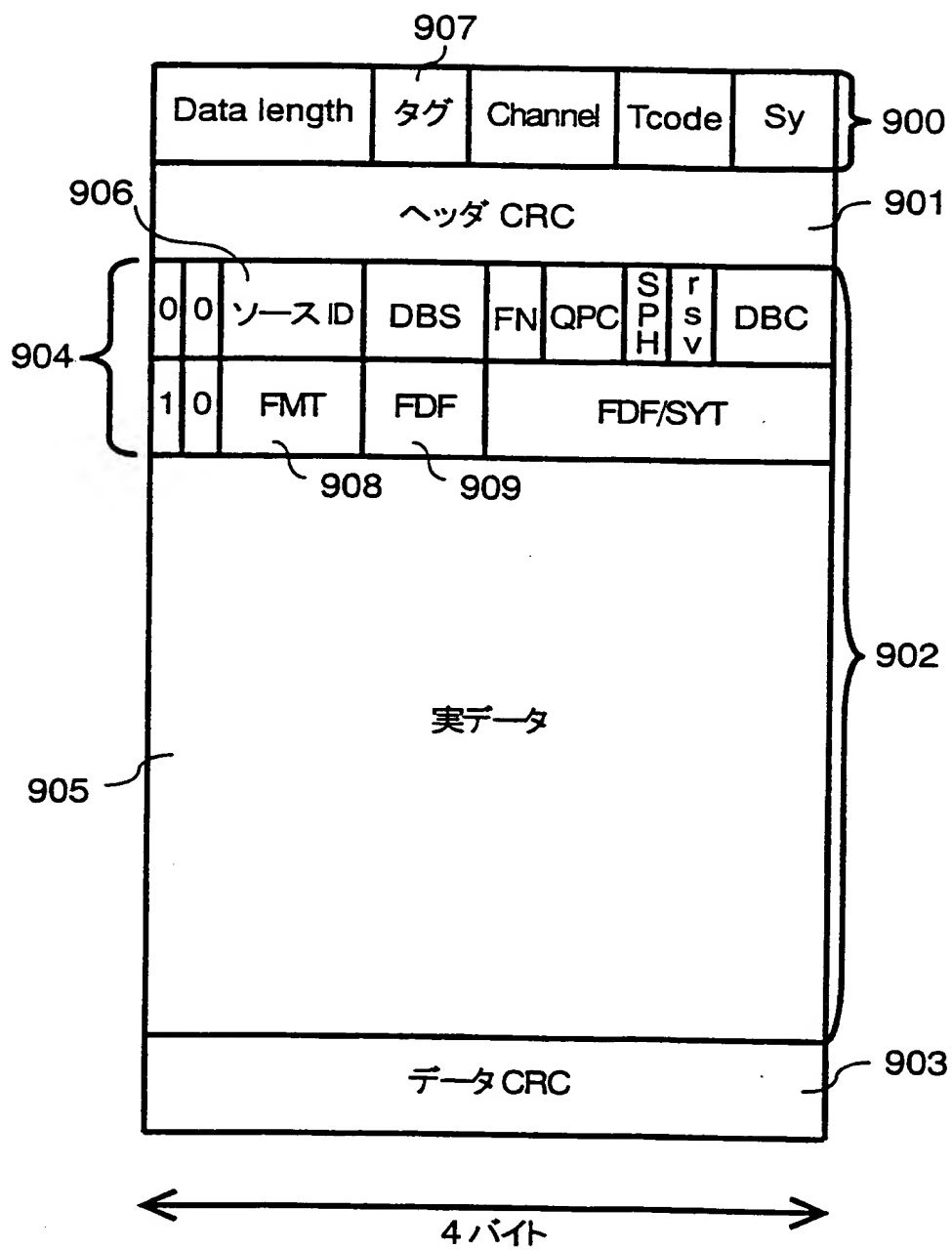


図 5

THIS PAGE BLANK (USPTO)

図面の参照符号の一覧表

100	信号源
101	暗号化手段
102	ソースパケット化手段
103	CIPぶろっく化手段
107	アイソクロノスパケット化手段
108、127	1394パケット入出力手段
105	出力命令
109、126	暗号鍵
110	送信装置
128	受信装置
111	IEEE1394バス
106、125	鍵生成手段
120	映像音声化手段
121	複合化手段
122	実データ抽出手段
123	ペイロード抽出手段
200	アルゴリズムID
201	アルゴリズム領域
202	ラベル
203	ステップ番号
204	チャネル番号
205	ブロック番号
206	総ブロック数
207	データ
208	オペコード
209	データ長

THIS PAGE BLANK (USPTO)

212 最大データ長
299 サブファンクション
300 AKEステイタスコマンド
301 AKEレスポンス
302、306 メイクレスポンスコマンド
303、305、307、309、311、313 応答
304、308 ベリファイミーコマンド
310 クリエイトキーインフォコマンド
312 リコンストラクトキーコマンド
900 アイソクロノスケットヘッダ
901 ヘッダCRC
902、952 アイソクロノスペイロード
903 データCRC
904、954 CIPヘッダ
905 実データ
906 ソースID
907 タグ
908 FMT
909 FDF
910 暗号化情報 (ENC)
952 アイソクロノスペイロード

THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)